

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-198776

(43)Date of publication of application : 31.07.1998

(51)Int.Cl.

G06K 19/07
G06K 17/00
G06K 19/10

(21)Application number : 09-017427

(71)Applicant : DAINIPPON PRINTING CO LTD

(22)Date of filing : 14.01.1997

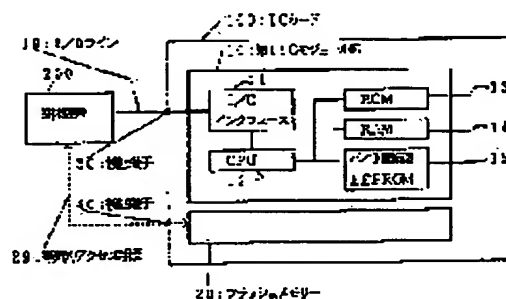
(72)Inventor : ISHIBASHI MASAKAZU

(54) PORTABLE INFORMATION RECORDING MEDIUM, AND ITS INFORMATION WRITING AND READING METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To make it possible to record a large amount of information, and also to improve the processing speed and security of a portable information recording medium, by recording the information to both 1st and 2nd IC modules containing the nonvolatile memories.

SOLUTION: An IC card 100 serves as a double chip type IC card, which contains a 1st IC module part 10 and a flash erasion type EEPROM (flash memory) 20 that is formed on the card surface as a 2nd IC module part. A contact terminal 30 is provided on the surface of the part 10. The card 100 is accessed by an exclusive terminal equipment 200. For instance, a byte rewrite type EEPROM 15 included in the part 10 of the card 100 has the memory capacity of only 8KB. On the other hand, the memory 20 can record the information of 8MB. Therefore, the card 100 can record a large quantity of information compared with an IC card provided with only the module part 10.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C): 1998,2003 Japan Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-198776

(43) 公開日 平成10年(1998) 7月31日

(51) Int.Cl.⁶

識別記号

F I

G 0 6 K 19/07
17/00
19/10G 0 6 K 19/00
17/00
19/00N
T
R

審査請求 未請求 請求項の数10 F D (全 15 頁)

(21) 出願番号 特願平9-17427

(22) 出願日 平成9年(1997) 1月14日

(71) 出願人 000002897

大日本印刷株式会社

東京都新宿区市谷加賀町一丁目1番1号

(72) 発明者 石橋 正教

東京都新宿区市谷加賀町一丁目1番1号

大日本印刷株式会社内

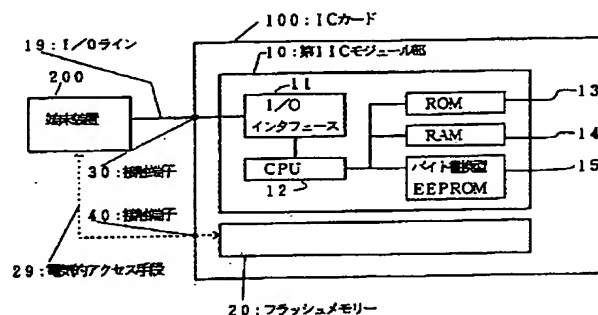
(74) 代理人 弁理士 小西 淳美

(54) 【発明の名称】 携帯可能情報記録媒体およびこれに対する情報書込／読出方法

(57) 【要約】

【課題】 2つのICモジュールに情報を記録することにより大容量の情報記録が可能で、処理速度の速い携帯可能情報記録媒体を提供し、かつ、セキュリティが非常に高く、情報の改ざんに対処する。

【解決手段】 CPUと、このCPUが実行するプログラムを記憶したROMと、CPUの作業領域として使用されるRAMと、CPUを介してデータの読出しおよび書き込みができる電氣的に消去・再書き込み可能な不揮発性メモリと、を有する第一ICモジュールと、電氣的に消去・再書き込み可能な不揮発性メモリからなる第二ICモジュールと、を搭載し、第一ICモジュール内と第二ICモジュール内との双方に情報記録を行うことができる携帯可能情報記録媒体である。



【特許請求の範囲】

【請求項 1】 CPUと、このCPUが実行するプログラムを記憶したROMと、前記CPUの作業領域として使用されるRAMと、前記CPUを介してデータの読出しおよび書き込みができる電氣的に消去・再書き込み可能な不揮発性メモリと、を有する第一ICモジュールと、
電氣的に消去・再書き込み可能な不揮発性メモリからなる第二ICモジュールと、を搭載し、
前記第一ICモジュール内と前記第二ICモジュール内との双方に情報記録を行うことができる携帯可能情報記録媒体。

【請求項 2】 前記第一ICモジュール内の不揮発性メモリがバイト書換型EEPROMであり、前記第二ICモジュール内の不揮発性メモリがフラッシュ消去型EEPROMであることを特徴とする請求項 1 記載の携帯可能情報記録媒体。

【請求項 3】 前記第一ICモジュール内に対して外部から所定のデータが与えられたときに、前記第一ICモジュール内の不揮発性メモリ内に記録されている暗号化キーを用いて、前記データから一義的に導出される認証コードを生成する認証コード生成処理を前記CPUが実行できるように、認証コード生成プログラムを前記ROM内に用意したことを特徴とする請求項 1、2 記載の携帯可能情報記録媒体。

【請求項 4】 請求項 3 に記載の媒体において、与えられたデータを n 個 ($n \geq 2$) のブロックに分割し、この n 個のブロックに m 個の暗号化キー ($m \geq 1$) を加えた ($n+m$) 組のデータのすべてが関与した相互論理演算を行い、前記与えられたデータのデータ長よりも短い認証コードを生成することができる認証コード生成プログラムを用意したことを特徴とする携帯可能情報記録媒体。

【請求項 5】 請求項 3 または 4 に記載の媒体において、
第一ICモジュール内で生成された認証コードを、この認証コードのもととなったデータに付加して、第二ICモジュール内に記録したことを特徴とする携帯可能情報記録媒体。

【請求項 6】 請求項 3～5 のいずれかに記載の媒体において、
第一ICモジュールに接続されている端末装置が正規のものであるか否かを判定する機能を第一ICモジュールに用意し、正規の端末装置であった場合にのみ、認証コード生成処理が実行されるようにしたことを特徴とする携帯可能情報記録媒体。

【請求項 7】 CPUと、このCPUによってアクセスされる第一メモリと、電氣的に消去・再書き込み可能な不揮発性メモリからなる第二メモリとを有し、前記第一メモリと前記第二メモリとの双方に情報記録を行うこと

ができる携帯可能情報記録媒体に対する情報書込方法であって、

前記第二メモリへ書込むべき記録対象データを用意し、
前記第一メモリ内に記録されている暗号化キーを用いて、前記記録データから一義的に導出される認証コードを生成する認証コード生成処理を前記CPUによって実行させ、
生成された認証コードを前記記録対象データに付加して前記第二メモリへ書込むようにしたことを特徴とする携帯可能情報記録媒体に対する情報書込方法。

【請求項 8】 請求項 7 に記載の情報書込方法において、

第二メモリに記録されている暗号化キーを、この媒体に接続されている端末装置についてのホストコンピュータ内にも用意し、認証コード生成処理を前記媒体内のCPUに実行させる代わりに、前記ホストコンピュータに実行させることを特徴とする携帯可能情報記録媒体に対する情報書込方法。

【請求項 9】 請求項 7 または 8 に記載の方法によって第二メモリに書込まれた情報を読み出す方法であって、第二メモリに書込まれている記録対象データおよび認証コードを読出し、媒体の第一メモリ内に記録されている暗号化キーを用いて、前記記録対象データから一義的に導出される認証コードを生成する認証コード生成処理を前記CPUによって実行させ、

第二メモリから読み出された認証コードと、前記認証コード生成処理で生成された認証コードとを比較し、両者が一致している場合にのみ、第二メモリから読み出された記録対象データを正しいデータとして取り扱うことを特徴とする携帯可能情報記録媒体に対する情報読出方法。

【請求項 10】 請求項 9 に記載の情報読出方法において、

第二メモリ内に記録されている暗号化キーを、この媒体に接続されている端末装置についてのホストコンピュータ内にも用意し、認証コード生成処理を前記媒体内のCPUに実行させる代わりに、前記ホストコンピュータに実行させることを特徴とする携帯可能情報記録媒体に対する情報読出方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は携帯可能情報記録媒体およびこれに対する情報書込／読出方法に関し、特にCPUとメモリを有するICモジュールを1つ目とし、電氣的に消去・再書き込み可能な不揮発性メモリからなるICモジュールを2つ目として搭載された、いわゆる2チップ型のICカードなどに対して利用するのに適した情報の書込／読出方法に関する。

【0002】

【従来の技術】 携帯可能情報記録媒体として、現在、磁

気カードが広く普及しているが、大きな記憶容量を確保できる光カードや十分なセキュリティを確保できるICカードも実用化されている。今後は、半導体集積回路の小型化、低コスト化のための技術進歩により、実社会の種々のシステムにおいてICカードが利用されるものと思われる。

【0003】特に、CPUを内蔵したICカードでは、単なる情報記録媒体としての機能だけではなく、情報処理機能が付加されるため、高度なセキュリティを必要とする情報処理システムへの利用が期待されている。現在普及している一般的なICカードは、CPUと、このCPUによってアクセスされる3種類のメモリ、すなわち、ROM、RAM、EEPROMを有している。ROM内には、CPUによって直接実行可能なインストラクションコードからなるプログラムが記憶されており、CPUはこのプログラムに基づいて、ICカードを統括制御する機能を有する。RAMは、CPUがこのような統括制御を行う上での作業領域として使用されるメモリである。一方、EEPROMは、CPUを介してデータの読出しおよび書き込みが可能な不揮発性メモリであり、このICカードに記録すべき本来のデータを格納するために用いられる。

【0004】光カードでは、表面に情報記録部が設けられており、光学的読取装置を用いることにより、この情報記録部に記録されたデジタルデータを読み取ることが可能である。このため、不正な手段による読出しも比較的容易に行いうる。これに対して、ICカードに内蔵されているEEPROMへのアクセスは、すべてCPUを介して行われ、外部からEEPROMを直接アクセスすることはできない。したがって、ICカードは、光カードに比べて高度なセキュリティを確保することが可能になる。そこでICメモリによる記録と、光記録、光磁気記録などの光を用いた記録とを併用したいわゆる「ハイブリッド型」の情報記録カードが提案されている。

【0005】たとえば、光記録を併用したハイブリッドICカードでは、カード状の媒体内部にICモジュールが埋め込まれるとともに、表面に光記録部が形成される。このようなハイブリッドICカードを用いれば、記録すべき情報は、ICモジュール内のEEPROMへデジタルデータとして記録することもできるし、光記録部にデジタルビットとして記録することもできる。そこで、高度なセキュリティを要する情報についてはEEPROMへ記録し、大容量の情報については光記録部へ記録する、という利用形態が可能となる。

【0006】

【発明が解決しようとする課題】しかし、上述したハイブリッドICカードでは、光記録部へ大容量の情報を記録することが可能になるが、光記録部は、その書き込みや読み取りにおいて、カードの上下あるいは左右の方向に直線状にしか記録できず、したがって光学的読取装置

の読取り部を上下あるいは左右方向に往復動することでは書き込みや読み取りができないものであり、処理速度が遅く、時間を非常に要し、かつリダライタをコンパクトにできないものであった。また、その記録に関しても追記のみであり、書換えが不可能なもので、かつ表面に傷などがつき易い等の欠点も有するものであった【0007】また、光記録部に記録された情報に対するセキュリティは低いものであり、そこで、秘密にする必要性の低い情報を光記録部へ記録するのが一般的な利用形態となる。すなわち、万一、不正な手段によって読み取られることがあっても、重大な事態にはならないような情報を光記録部へ記録するようにすれば、不正読み取りによるセキュリティ上の大きな問題は解決できる。ところが、不正な手段による書き込みが行われると、利用上、大きな問題が生じることになる。すなわち、不正書き込みを行えば、記録データを改ざんすることが可能であり、このようなデータ改ざんが行われると、ICカードを利用した運用システム全体に大きな支障を生じる可能性がある。光記録部に記録された情報は、微小なデータビットの有無によって1ビットを表現した情報であり、新たなデータビットを生成することにより比較的容易に改ざんが可能である。光磁気記録部に記録された情報も同様に改ざんされる可能性がある。

【0008】そこで本発明は、CPUを有するICモジュールと、それ以外のカード表面に電氣的に消去・再書き込み可能な不揮発性メモリからなる別のICモジュールとを搭載し、その双方のICモジュールに情報を記録することのできる、大容量の情報記録が可能で、処理速度の速い携帯可能情報記録媒体を提供するとともに、その記録情報に対するセキュリティの非常に高い、情報記録部に記録された情報の改ざんに対処することを目的とする。

【0009】

【課題を解決するための手段】

(1) 本発明の第1の態様は、CPUと、このCPUが実行するプログラムを記憶したROMと、CPUの作業領域として使用されるRAMと、CPUを介してデータの読出しおよび書き込みができる電氣的に消去・再書き込み可能な不揮発性メモリと、を有する第一ICモジュールと、電氣的に消去・再書き込み可能な不揮発性メモリからなる第二ICモジュールと、を搭載し第一ICモジュール内と第二ICモジュール内との双方に情報記録を行うことができる携帯可能情報記録媒体である。

【0010】(2) 本発明の第2の態様は、第一ICモジュール内の不揮発性メモリがバイト書換型EEPROMであり、第二ICモジュールの不揮発性メモリがフラッシュ消去型EEPROMであることを特徴とするものである。

【0011】(3) 本発明の第3の態様は、第一ICモジュール内に対して外部から所定のデータが与えられたと

きに、第一ICモジュール内の不揮発性メモリ内に記録されている暗号化キーを用いて、データから一義的に導出される認証コードを生成する認証コード生成処理をCPUが実行できるように、認証コード生成プログラムをROM内に用意したものである。

【0012】(4) 本発明の第4の態様は、上述の第3の態様に係る携帯可能情報記録媒体において、与えられたデータを n 個($n \geq 2$)のブロックに分割し、この n 個のブロックに m 個の暗号化キー($m \geq 1$)を加えた($n+m$)組のデータのすべてが関与した相互論理演算を行い、前記与えられたデータのデータ長よりも短い認証コードを生成することができるようにしたものである。

【0013】(5) 本発明の第5の態様は、上述の第3または第4の態様に係る携帯可能情報記録媒体において、第一ICモジュール内で生成された認証コードを、この認証コードのもととなったデータに付加して、第二ICモジュール内に記録したものである。

【0014】(6) 本発明の第6の態様は、上述の第3～5の態様に係る携帯可能情報記録媒体において、第一ICモジュールに接続されている端末装置が正規のものであるか否かを判定する機能を第一ICモジュールに用意し、正規の端末装置であった場合にのみ、認証コード生成処理が実行されるようにしたものである。

【0015】(7) 本発明の第7の態様は、CPUと、このCPUによってアクセスされる第一メモリと、電氣的に消去・再書き込み可能な不揮発性メモリからなる第二メモリとを有し、第一メモリと第二メモリとの双方に情報記録を行うことができる携帯可能情報記録媒体に対する情報書込方法であって、第二メモリへ書込むべき記録対象データを用意し、第一メモリ内に記録されている暗号化キーを用いて、記録データから一義的に導出される認証コードを生成する認証コード生成処理をCPUによって実行させ、生成された認証コードを記録対象データに付加して第二メモリへ書込むようにしたものである。

【0016】(8) 本発明の第8の態様は、上述の第7の態様に係る携帯可能情報記録媒体に対する情報書込方法において、第二メモリに記録されている暗号化キーを、この媒体に接続されている端末装置についてのホストコンピュータ内にも用意し、認証コード生成処理を媒体内のCPUに実行させる代わりに、ホストコンピュータに実行させるようにしたものである。

【0017】(9) 本発明の第9の態様は、上述の第7または第8の態様に係る方法によって情報記録部に書込まれた情報を読み出す方法において、第二メモリに書込まれている記録対象データおよび認証コードを読出し、媒体の第一メモリ内に記録されている暗号化キーを用いて、記録対象データから一義的に導出される認証コードを生成する認証コード生成処理を前記CPUによって実行させ、第二メモリから読み出された認証コードと、認証コード生成処理で生成された認証コードとを比較し、

両者が一致している場合にのみ、第二メモリから読み出された記録対象データを正しいデータとして取り扱うようにしたものである。

【0018】(10) 本発明の第10の態様は、上述の第9の態様に係る携帯可能情報記録媒体に対する情報読出方法において、情報記録部内に記録されている暗号化キーを、この媒体に接続されている端末装置についてのホストコンピュータ内にも用意し、認証コード生成処理を前記媒体内のCPUに実行させる代わりに、ホストコンピュータに実行させるようにしたものである。

【0019】そこで本発明は、CPUを有するICモジュールと、それ以外のカード表面に電氣的に消去・再書き込み可能な不揮発性メモリからなる別のICモジュールとを搭載し、その双方のICモジュールに情報を記録することのできる、大容量の情報記録が可能で、処理速度が速く、かつ表面物性に優れた携帯可能情報記録媒体を提供するとともに、その記録情報に対するセキュリティの非常に高い、電氣的に消去・再書き込み可能な不揮発性メモリからなるICモジュールに記録された情報の改ざんに対処することを目的とする。

【0020】

【作用】本発明に係る携帯可能情報記録媒体では、CPUを有するICモジュールと、それ以外のカード表面に電氣的に消去・再書き込み可能な不揮発性メモリからなる別のICモジュールとの双方に情報を記録することができるので、大容量の情報記録を可能とし、処理速度においても非常に速く、表面物性に優れたものとすることができる。

【0021】また、CPUを有する第一ICモジュールのメモリに、暗号化キーが用意され、内蔵CPUによってこの暗号化キーを用いた認証コード生成処理を実行する機能が付加されている。そこで、電氣的に消去・再書き込み可能な不揮発性メモリからなる第二ICモジュールへ記録すべきデータに対して認証コードを生成し、生成した認証コードをもとのデータに付加した状態で書き込みを行えば、読出し時には、この認証コードの整合性をチェックすることにより、データに対する改ざんの有無を認識することができる。

【0022】たとえば、2チップ型ICカードの表面の電氣的に消去・再書き込み可能な不揮発性メモリからなる第二ICモジュールにデータDを書込む場合は、このデータDに対して、第二ICモジュール内で所定の暗号化キーを用いた認証コード生成処理を実行し、認証コードCを生成する。そして、データDに認証コードCを付加した形で、第二ICモジュールに書き込みを行う。一方、読出し時には、データDとともにコードCを読出し、このデータDと暗号化キーとに基づいて生成した認証コードと、読出したコードCとが一致するかどうかをチェックすればよい。第二ICモジュールに対する改ざんが行われていた場合には、このチェックにより不一致が

生じるため、改ざんを認識することができる。認証コード生成処理に用いられる暗号化キーは、CPUを有する第一ICモジュール内に記録されているため、不正な手段によってこの暗号化キーを外部へ読み出すことは非常に困難であり、不正な手段によって認証コードが生成される可能性は極めて低い。

【0023】もっとも、暗号化キーに対するセキュリティが十分に確保できる環境においては、暗号化キーを媒体の外部に用意し、認証コード生成処理を外部で行うことも可能である。たとえば、媒体をアクセスするための端末装置に接続されたホストコンピュータについて十分なセキュリティが得られるのであれば、このホストコンピュータ内に暗号化キーを用意して認証コード生成処理を実行できるようにしておけば、この認証コード生成処理をより短時間で実行できるメリットが得られる。

【0024】また、媒体の内部で認証コード生成処理を実行する場合、CPUを有する第一ICモジュールに接続されている端末装置が正規のものであるか否かを判定し、正規の端末装置で合った場合にのみ、認証コード生成処理が実行されるようにしておけば、セキュリティを更に向上させることができる。

【0025】

【発明の実施の形態】以下、本発明を図示する実施例に基づいて説明する。

【0026】§1. 2チップ型ICカードの構成

はじめに、2チップ型ICカードの構成を説明する。図1に外観を示すICカード100は、第一ICモジュール部10を内蔵し、表面に第二ICモジュール部としてフラッシュ消去型EEPROM20（以下、フラッシュメモリ20という）が形成された2チップ型ICカードである。第一ICモジュール部10の表面には、接触端子30が設けられている。このICカード100に対するアクセスは、専用の端末装置200によって行われる。端末装置200にICカード100を挿入すると、端末装置200内の電極と接触端子30とが電氣的に接触し、この接触端子30を介して、第一ICモジュール部10に対する電源供給、クロック供給、データの送受が行われることになる。また、端末装置200には、フラッシュメモリ20の表面に設けられた接触端子40を介して上記同様に電氣的に書き込んだり、フラッシュメモリ20内に電氣的に記録されている領域の情報を読み込んだりする電氣的アクセス手段が組み込まれている。

【0027】図2は、このICカード100を端末装置200に接続し、アクセスを行っている状態を示すブロック図である。ICカード100と端末装置200とはI/Oライン19および接触端子30を介して相互に接続されている。この他、端末装置200とICカード100との間には、電源・クロック・リセット信号などの供給路が形成されるが、ここではこれら供給路の図示は

省略する。

【0028】ICカード100に内蔵された第一ICモジュール部10には、I/Oインタフェース11、CPU12、ROM13、RAM14、バイト書換型EEPROM15が内蔵されている。I/Oインタフェース11は、I/Oライン19を介してデータを送受するための入力回路であり、CPU12はこのI/Oインタフェース11を介して、端末装置200と通信することになる。ROM13内には、CPU12によって実行されるプログラムが記憶されており、CPU12はこのプログラムに基いて、第一ICモジュール部10を統括制御する機能を有する。RAM14は、CPU12がこのような統括制御を行う上での作業領域として使用されるメモリである。一方、バイト書換型EEPROM15は、第一ICモジュール部10に記録すべき本来のデータを格納するメモリである。ICカード100が端末装置200と切り離されると、電源およびクロックの供給は停止する。このとき、RAM14内のデータは、電源供給の停止によりすべてが失われるが、バイト書換型EEPROM15は不揮発性メモリであるため、電源供給が停止した後もその記録内容はそのまま保持される。

【0029】端末装置200は、電氣的アクセス手段29によってフラッシュメモリ20の接続端子40に対するアクセスを行うこともできる。電氣的アクセス手段29は、上述した第一ICモジュール10とI/Oカードインターフェイスにより端末装置200と通信すると同様であり、フラッシュメモリ20内にデジタル情報の記録を行う。この実施例に係るICカード100では、第一ICモジュール部10内のバイト書換型EEPROM15は8KBの記録容量しかもたないのに対し、フラッシュメモリ20には8MBの情報記録が可能である。したがって、第一ICモジュール部10のみしか備えていないICカードに比べれば、この2チップ型ICカード100には大量の情報を記録することが可能である。

【0030】§2. 改ざん防止機能を有する認証コードの生成方法

一般に、何らかの媒体に記録されているデータに対して、改ざんが行われるおそれがある場合、認証コードに基づいて改ざんの有無を判断する方法が知られている。すなわち、予め秘密の暗号化キーを用意しておき、この暗号化キーを用いて、もとのデータから一義的に導出される認証コードを生成する。そして、もとのデータとともにこの認証コードをチェックすることにより、改ざんの有無を判断することができる。すなわち、データを認証コードとともに読出し、書込み時と同じ暗号化キーを用いて、読出したデータから一義的に導出される認証コードを生成し、この生成した認証コードと読出した認証コードとが一致するか否かを判断するのである。通常、両者は一致するはずであるから、万一、不一致が生じた場合

には、何らかの改ざんが行われたものと判断することができる。

【0031】このような認証コードは、一般にMAC (Message Authentication Code) と呼ばれている。MACは、もとのデータから一義的に定まるデータであればどのようなデータを用いてもかまわないが、通常は、データ記録の冗長度をある程度に抑えるために、もとのデータの長さよりもかなり小さなMACが利用される。MACに基づいて、逆にもとのデータを生成させる必要性はないので、もとのデータの情報量に対して、MACの情報量がある程度小さくても問題はない。ただし、MACはもとのデータの全般が関与する形で生成する必要がある。別言すれば、もとのデータの任意の1ビットに変化が生じた場合には、必ずMAC自身にも何らかの変化が現れるようにしておく必要がある。こうしておけば、いずれか1ビットでも改ざんされれば、MACの照合が一致しくなくなり、改ざんがあったことを認識することができる。

【0032】このような条件を満たす認証コードMACの生成方法としては、もとのデータをブロック分割して取り扱う方法が知られている。たとえば、もとのデータを n 個 ($n \geq 2$) のブロックに分割し、この n 個のブロックに m 個の暗号化キー ($m \geq 2$) を加えた ($n+m$) 組のデータのすべてが関与した相互論理演算を行い、もとのデータのデータ長よりも短い認証コードMACを生成するのである。

【0033】この方法の具体例を図3を参照しながら説明する。いま、図3の上部に示したように、所定の長さをもった「1区切りのデータ」に対して認証コードMACを生成する場合を考える。この場合、この「1区切りのデータ」を複数 n 個のブロックに分割する。この例では、1つのブロックのデータ長が8バイトとなるような分割が行われている。続いて、所定の暗号化キー K (例えば、8バイトのデータ) を用いて、暗号化手段31によってブロック1に対する暗号化処理を行い、その結果としてブロック1'を得る。暗号化手段31において実行する暗号化処理は、ブロック1と暗号化キー K とを用いた論理演算であればどのようなものでもかまわない。いずれにせよ、得られるブロック1'は、ブロック1と暗号化キー K とが特定されれば一義的に定まるデータになる。次に、演算器32によって、ブロック1'とブロック2との排他的論理和をとり、ブロック2'を求め、続いて、演算器33によって、ブロック2'とブロック3との排他的論理和をとり、ブロック3'を求める。以下、同様に、ブロック i 'とブロック($i+1$)との排他的論理和をとり、ブロック($i+1$)'を得る処理を $i=n-1$ になるまで繰り返し実行し、ブロック n 'を求めれば、このブロック n 'が生成すべき認証コードMACとなる。この例では、もとの「1区切りのデータ」が($8 \times n$)バイトの長さであったのに対して、得られ

た認証コード mac は8バイトの長さになる。

【0034】このような方法で生成された認証コードMACは、もとの「1区切りのデータ」と暗号化キー K とに基づいて一義的に導出されるコードであり、もとのデータ内のいずれか1ビットでも変更されると、異なった値をとる。なお、図3に示した認証コードMACの生成方法は、一例を示したものであり、本発明は、このような認証コードMACの生成方法に限定されるものではない。例えば、ブロック2'と暗号化キー K とに基づいてブロック3'を得るようにしてもよいし、演算器32として他の論理演算を行うようにしてもよいし、暗号化キー K_1 、 K_2 、...と複数のキーを用いるようにしてもよい。要するに、与えられたデータと予め用意した暗号化キーとに基づいて一義的に定まるようなコードであれば、どのようなコードを認証コードMACとして用いてもかまわない。

【0035】§3. セキュリティを有する2チップ型ICカード

続いて、本発明のセキュリティを有する2チップ型ICカードの構成と、このICカードの第2ICモジュール部としてのフラッシュメモリーに対するデータの書込処理および読出処理を説明する。図4は、本発明の一実施例に係る2チップ型ICカード100を端末装置200に接続し、アクセスを行っている状態を示すブロック図であり、そのハードウェア構成は、図2において述べた2チップ型ICカードと同様である。ただ、ROM13内にMAC生成ルーチンが付加され、バイト書換型EEPROM15内に暗号化キー K が記録されている点と異なり、また、フラッシュメモリー20内に記録される「1区切りのデータ」には、認証コードMACが付加される点と異なる。

【0036】はじめに、図5の流れ図を参照しながら、この図4に示す2チップICカード100についてのフラッシュメモリー20へのデータ書込処理の手順を説明する。なお、この流れ図において、ステップS11、S12、S16は端末装置200側でフラッシュメモリー20への記録すべき記録対象データを用意する。この記録対象データは、図3における「1区切りのデータ」に対応するものである。認証コードMACの長さに比べて、「1区切りのデータ」の長さが長ければ、それだけ認証の精度が低下するので、この「1区切りのデータ」の長さは、必要な認証精度を考慮の上、適宜設定しておくようにする。

【0037】続くステップS12では、ステップS11で用意したデータをMAC生成コマンドとともに第一ICモジュール部10へと転送する。このように、「コマンド」の形式で、端末装置200から第一ICモジュール部10へデータを転送するのは、端末装置200と第一ICモジュール部10との間の交信が、「コマンド」とそれに対する「レスポンス」という形で行われるから

である。すなわち、端末装置200からCPU12に対して所定の「コマンド」を与えると、CPU12はこの「コマンド」を解釈し、ROM13内に用意されているこのコマンドに対応したルーチンを実行し、その結果を、端末装置200に対して「レスポンス」として返送することになる。例えば、バイト書換型EEPROM15内の所定のファイルに書き込みを行う場合には、「書込コマンド」とともに書込対象となるデータをCPU12に与え、CPU12による「書込コマンド」の実行という形式で書込処理が行われることになる。逆に、バイト書換型EEPROM15内の所定のファイルからデータの読出しを行う場合は、所定の「読出コマンド」をCPU12に与え、CPU12による「読出コマンド」の実行という形式で読出処理が行われることになる。このように、第一ICモジュール10内において「コマンド」の実行が終了すると、実行した「コマンド」に対する「レスポンス」が外部に対して返送される。例えば、「書込コマンド」を与えた場合には、書込処理が支障なく実行されたか否かを示す「レスポンス」返送され、「読出コマンド」を与えた場合には、読出対象となったデータがレスポンスという形で返送されることになる。そこで、ステップS12では、認証コードMACを生成する指示を与える「MAC生成コマンド」とともに、ステップS11で用意した記録対象データ（図3の「1区切りのデータ」）に対応するデータを第一ICモジュール部10へ与えている。

【0038】第一ICモジュール部10は、このようなコマンドを解釈し、ROM13内に用意されたMAC生成ルーチンを利用して、次のような処理を実行する。まず、この実施例では、MAC生成ルーチンの実質的な処理に入る前に、ステップS13において、現在接続されている端末装置200が正規の端末装置として認証済みであるか否かがチェックされる。通常、ICカード100を端末装置200に挿入し、両者を電氣的に接続すると、相互に相手方が正しいものであるか否かを確認する相互認証処理が実行される。このような相互認証処理の具体的な方法については、既に公知の技術であるのでここでは説明を省略するが、この相互認証の結果、ICカード100側が相手（端末装置200）を正しいものと認証すると、通常は、RAM14内の「相手が正規の端末装置であることを示すフラグ」をセットする処理が行われる。この実施例では、ステップS13において、まずこのフラグがセットされていることを確認した後、MAC生成ルーチンを実行するようにしている。これは、セキュリティを更に向上させるための配慮であり、そのメリットについては後述する。

【0039】さて、ステップS13において、現在接続されている端末装置200が正規の端末装置であることが確認できたら、続くステップS14において、認証コードMACを生成する処理が行われる。すなわち、端末

装置200からコマンドとともに与えられた記録対象データ（図3の「1区切りのデータ」）とバイト書換型EEPROM15内に用意されている暗号化キーKとに基づいて一義的に導出される何らかのコードが生成される。この実施例では、図3に示す方法によって、認証コードMACが生成される。こうして認証コードMACが生成されたら、これをステップS15においてレスポンスとして端末装置200側へ返送する。

【0040】結局、端末装置200側から上述の処理を見ると、ステップS12において、コマンドとともに記録対象データをI/Oライン19を介して転送すると、ステップS15において、同じくI/Oライン19を介してレスポンスが得られたことになり、このレスポンスには、転送した記録対象データについての認証コードMACが含まれていることになる。そこで、端末装置200は、ステップS16において、用意した記録対象データ（「1区切りのデータ」）に、レスポンスとして戻された認証コードMACを付加し、これを電氣的アクセス手段29を介してフラッシュメモリ20内に書込む処理を行う。かくして、図4に示すように、フラッシュメモリ20内には、「1区切りのデータ」が認証コードMACとともに書込まれることになる。

【0041】なお、ステップS13において、現在接続されている端末装置200が正規の端末装置ではないと判断された場合、すなわち、相互認証処理が正常に完了したことを示すフラグがRAM14内にセットされていなかった場合は、ステップS17において、エラーレスポンスが返送される。したがって、たとえば、不正な端末装置によってICカード100と交信し、この不正な端末装置からMAC生成コマンドを与えたとしても、ICカード100からはエラーレスポンスが戻ることになり、認証コードMACを得ることはできない。したがって、不正な端末装置を用いて、特定のデータについての認証コードMACを知得するような不正行為は拒絶され、十分なセキュリティを確保することが可能になる。もちろん、ステップS13の判断処理は、本発明を実施する上で必要不可欠の処理ではないが、実用上、十分なセキュリティを確保する上では、この処理を実行するのが好ましい。

【0042】続いて、図6の流れ図を参照しながら、図4に示す2チップ型ICカード100についてのフラッシュメモリ20からのデータ読出処理の手順を説明する。なお、この流れ図において、ステップS21、S22は端末装置200において行われる処理であり、ステップS23～S27はICカード100において行われる処理である。まず、ステップS21において、フラッシュメモリ20から電氣的アクセス手段29を介して、MAC付データの読出しが行われる。すなわち、図4のフラッシュメモリ20に示す「1区切りのデータ」と認証コードMACとが1組のデータとして、端末

装置 200 側に読み出されることになる。

【0043】続くステップ S22 では、ステップ S21 で読出したデータを MAC 照合コマンドとともに第一 IC モジュール部 10 へと転送する。第一 IC モジュール部 10 は、このようなコマンドを解釈し、ROM13 内に用意された MAC 生成ルーチンを利用して、次のような処理を実行する。まず、この実施例では、MAC 生成ルーチンの実質的な処理に入る前に、ステップ S23 において、現在接続されている端末装置 200 が正規の端末装置として認証済みであるか否かがチェックされる。これは、前述したステップ S13 の処理と同様である。現在接続されている端末装置 200 が正規の端末装置であることが確認できたら、続くステップ S24 において、認証コード MAC を照合する処理が行われる。すなわち、端末装置 200 からコマンドとともに与えられたデータを、本来のデータ部分と認証コード MAC の部分とに分割し、本来のデータ部分（図 3 の「1 区切りのデータ」に相当）とバイト書換型 EEPROM15 内に用意されている暗号化キー K とに基づいて、認証コード MAC を生成する。この実施例では、図 3 に示す方法によって、認証コード MAC が生成される。こうして認証コード MAC が生成されたら、この生成された認証コード MAC と、端末装置 200 から与えられた認証コード MAC と、が一致するか否かを判断する。

【0044】フラッシュメモリー 20 内に記録されていた情報が、書込み時のままであれば、ステップ S25 における照合結果は一致を示すはずであるが、何らかの改ざんが行われていた場合には不一致を示すことになる。そこで、照合結果が一致すれば、ステップ S26 において正常レスポンスを返送し、不一致であれば、ステップ S27 においてエラーレスポンスを返送する。端末装置 200 側では、このレスポンスに基づいて、フラッシュメモリー 20 から読出したデータに対する改ざんの有無を認知することができるすなわち、正常レスポンスが得られた場合には、読出したデータを正しいデータとして取り扱うことができ、エラーレスポンスが得られた場合には、読出したデータには不正な改ざんが行われているとの認識のもとにしかるべき取扱を行うことができる。

【0045】なお、ステップ S23 において、正規の端末装置ではないと判断された場合、すなわち、相互認証処理が正常に完了したことを示すフラグが RAM14 内にセットされていなかった場合は、ステップ S27 において、エラーレスポンスが返送される。したがって、たとえば、不正な端末装置によって IC カード 100 と交信し、この不正な端末装置から MAC 照合コマンドを与えたとしても、IC カード 100 からはエラーレスポンスが戻ることであり、照合結果を得ることはできない。したがって、不正な端末装置を用いて、特定のデータと認証コード MAC との組み合わせについての照合結果を知得するような不正行為は拒絶され、十分なセキュリ

ティを確保することが可能になる。もちろん、ステップ S23 の判断は、本発明を実施する上で必要不可欠の処理ではないが、実用上、十分なセキュリティを確保する上では、この処理を実施するのが好ましい。

05 【0046】§ 4. 本発明の変形例

最後に、本発明の変形例を示す。図 7 は、これまで述べてきた本発明の IC カード 100 を用いた取引システムの一例を示すブロック図である。ここでは、2 つの端末装置に 201 と 202 と 4 枚の IC カード 101 ~ 104 とを用いた非常に単純なモデルを示してあるが、実際には、より多くの端末装置および IC カードが用いられる。このようなシステムでは、4 枚の IC カード 101 ~ 104 は、端末装置 201、202 のいずれにも接続可能である。たとえば、第 1 の IC カード 101 のフラッシュメモリー、第 1 の端末装置 201 を用いて所定のデータを書き込んだ場合、このデータは、第 2 の端末装置 202 によっても何ら支障なく読みだすことができる。なぜなら、認証コード MAC を生成するために用いられる暗号化キー K1 は、IC カード 101 内に用意されており、かつ、MAC 生成ルーチンも IC カード 101 内に用意されているので、どの端末装置を用いても同じ結果が得られるからである。したがって、本発明は、図 7 に示すような取引システムに何ら支障なく適用可能である。

25 【0047】図 8 は、図 7 に示す取引システムに、更に第 3 の端末装置 203 および第 4 の端末装置 204 を付加したものである。ここで、第 3 の端末装置 203 および第 4 の端末装置 204 は、いずれもホストコンピュータ 300 に接続されている。図 7 に示す第 1 の端末装置 201 および第 2 の端末装置 202 は、いずれもいわゆる「スタンドアロン型」のものであり、ホストコンピュータ 300 には接続されていない。これに対し、図 8 に示す第 3 の端末装置 203 および第 4 の端末装置 204 は、いずれもいわゆる「ネットワーク型」のものであり、ホストコンピュータ 300 に対してオンライン接続されている。

【0048】実社会における取引システムでは、しばしばこのような「スタンドアロン型」の端末装置と「ネットワーク型」の端末装置を混在させた形態が見られる。たとえば、銀行システムの場合、各支店等の比較的大規模な営業所には「ネットワーク型」の端末装置を設け、駅や百貨店の一角には「スタンドアロン型」の端末装置を設置するような利用形態が考えられる。本発明における「端末装置」という文言は、「スタンドアロン型」の装置と「ネットワーク型」の装置とを含んだ広い概念で用いられており、本発明は、図 7 の取引システムにも図 8 の取引システムにも、いずれにも適用可能である。

【0049】ただ、図 8 のような「ネットワーク型」の端末装置を含むシステムにも適用する場合、MAC 生成

処理やMAC照合処理をホストコンピュータ300側で行うことも可能である。即ち、各ICカード101～104のROM内に用意されたMAC生成ルーチンおよび第一ICモジュールのバイト書換型EEPROM内に用意された暗号化キーK1、K2、K3、K4を、ホストコンピュータ300内に用意しておくようにすれば、前述の実施例においてICカード内で実施していたMAC生成処理（ステップS13）やMAC照合処理（ステップS24）をホストコンピュータ300側で実行することも可能になる。

【0050】このような処理をホストコンピュータ300側で行うと、処理時間を短縮出来るといふメリットが得られる。即ち、個々のICカードに内蔵されたCPUと、ホストコンピュータ300内のCPUとを比較すると、両者のコストを比較すれば明らかなように、前者の演算処理能力は、後者の演算処理能力に比べれば非常に劣るものである。このため、例えば図3に示すような演算処理をICカード側のCPUに実行させればかなりの時間が必要になるのに対し、ホストコンピュータ300側のCPUに実行させれば瞬時に演算は完了する。また、これらの処理をICカード側のCPUに実行させるためには、端末装置からI/Oライン19を介してコマンドという形式でデータを転送する必要があり、この転送作業にもある程度の時間が必要になり、ICカード側での処理をさらに遅くする要因となっている。そこで、図8に示す端末装置203、204のように、ホストコンピュータ300に対してオンライン接続されている端末装置を用いてICカード100をアクセスしている場合には、MAC生成処理やMAC照合処理を、ICカード側で行う代わりに、ホストコンピュータ300側で行うと、全体の処理時間が短縮される。ただ、MAC生成ルーチンや個々のICカードについての暗号化キーK1～K4をホストコンピュータ300内に用意するため、十分なセキュリティを確保する必要がある。また、ホストコンピュータ300内でMAC生成処理やMAC照合処理を実行する前に、ホストコンピュータ・端末装置・ICカードの三者間において、互いに相手が正規のものであることを確認する相互認証がおこなわれていることを確認するようにすれば、不正アクセスに対しても十分なセキュリティ確保が実現できる。

【0051】以上、本発明を図示する実施例に基づいて説明したが、本発明はこれらの実施例に限定されるものではなく、この他にも種々の態様で実施可能である。たとえば、上述の実施例では、第二ICモジュール部にフラッシュメモリーを例にとって説明を行ったが、バイト書換型EEPROMを用いてもよく、また、その逆に第一ICモジュール部内のバイト書換型EEPROMにフラッシュメモリーを用いてもよいものである。さらに、バイト書換型EEPROMはその最小単位のビット単位にて書換・消去可能なビット書換型EEPROMとして

もちろん構わないものである。

【0052】

【発明の効果】以上のとおり本発明によれば、CPUを有するICモジュールと、それ以外のカード表面に電氣的に消去・再書き込み可能な不揮発性メモリからなる別のICモジュールとを搭載したICカードとすることにより、その双方のICモジュールに情報を記録することのできる、大容量の情報記録が可能で、処理速度が速く、かつ表面物性に優れた携帯可能情報記録媒体を提供するとともに、その記録情報に対するセキュリティの非常に高い、電氣的に消去・再書き込み可能な不揮発性メモリからなるICモジュールに記録された情報の改ざんに対する有効な対策をも実現できる。

【図面の簡単な説明】

【図1】ICモジュール部10およびフラッシュメモリー20を搭載した2チップ型ICカードの外観図である。

【図2】図1のICカード100を端末装置200に接続し、アクセスを行っている状態を示すブロック図である。

【図3】認証コードMACの生成方法の一例を示す図である。

【図4】本発明の一実施例に係る2チップ型ICカード100を端末装置200に接続し、アクセスを行っている状態を示すブロック図である。

【図5】図4に示す2チップ型ICカード100についてのフラッシュメモリー20へのデータ書込処理の手順を説明する流れ図である。

【図6】図4に示す2チップ型ICカード100についてのフラッシュメモリー20からの読出処理の手順を説明する流れ図である。

【図7】本発明に係るICカードとスタンドアロン型端末装置を用いた取引システムの一例を示すブロック図である。

【図8】本発明に係るICカードとネットワーク型端末装置を用いた取引システムの一例を示すブロック図である。

【符号の説明】

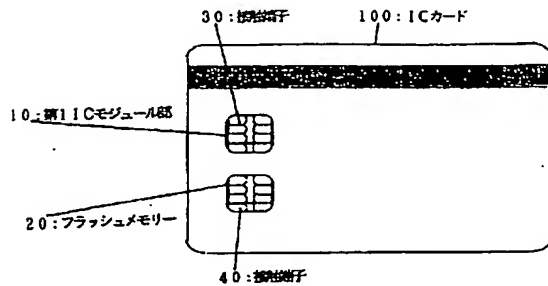
10	ICモジュール部
11	I/Oインタフェース
12	CPU
13	ROM
14	RAM
15	バイト書換型EEPROM
19	I/Oライン
20	フラッシュメモリー
29	電氣的アクセス手段
30	接触端子
31	暗号化手段
40	接触端子

100~104

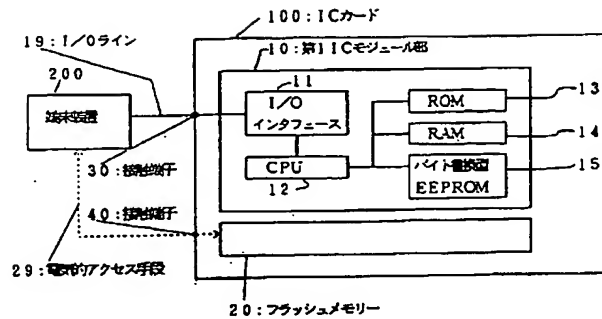
200~204

300

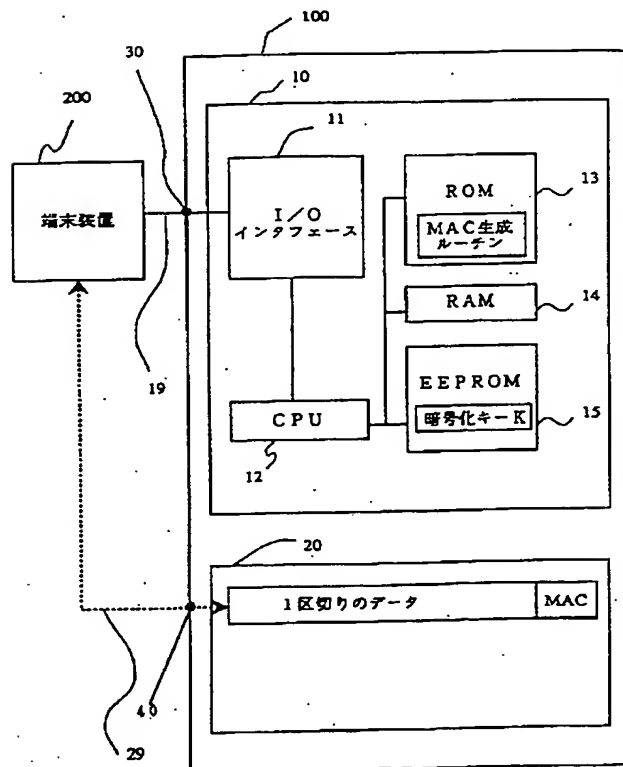
【図1】



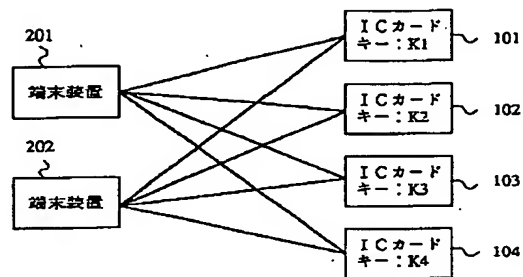
【図2】



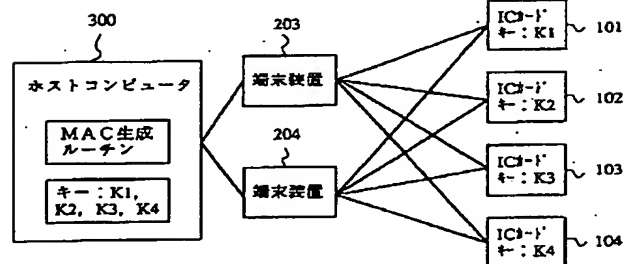
【図4】



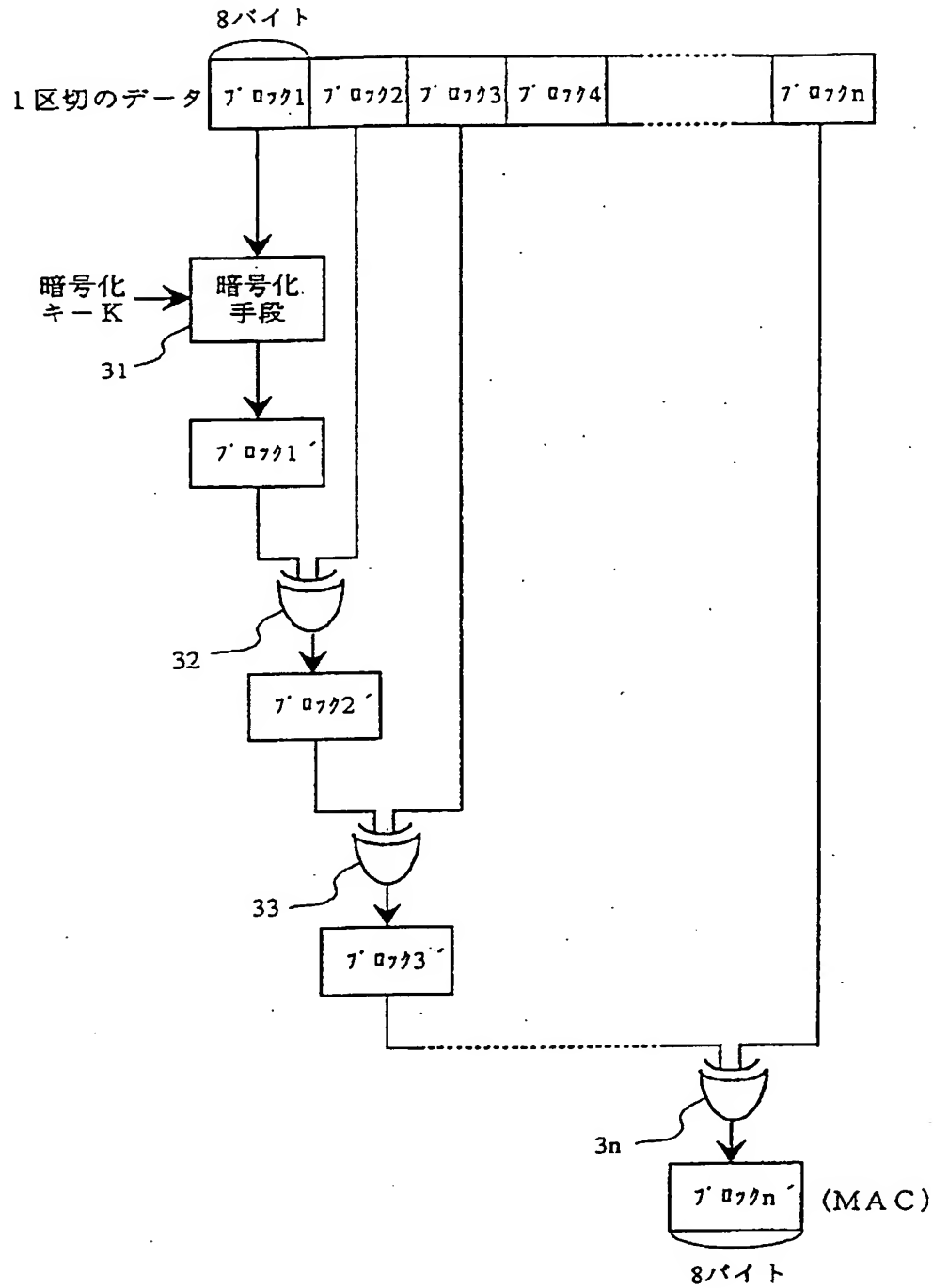
【図7】



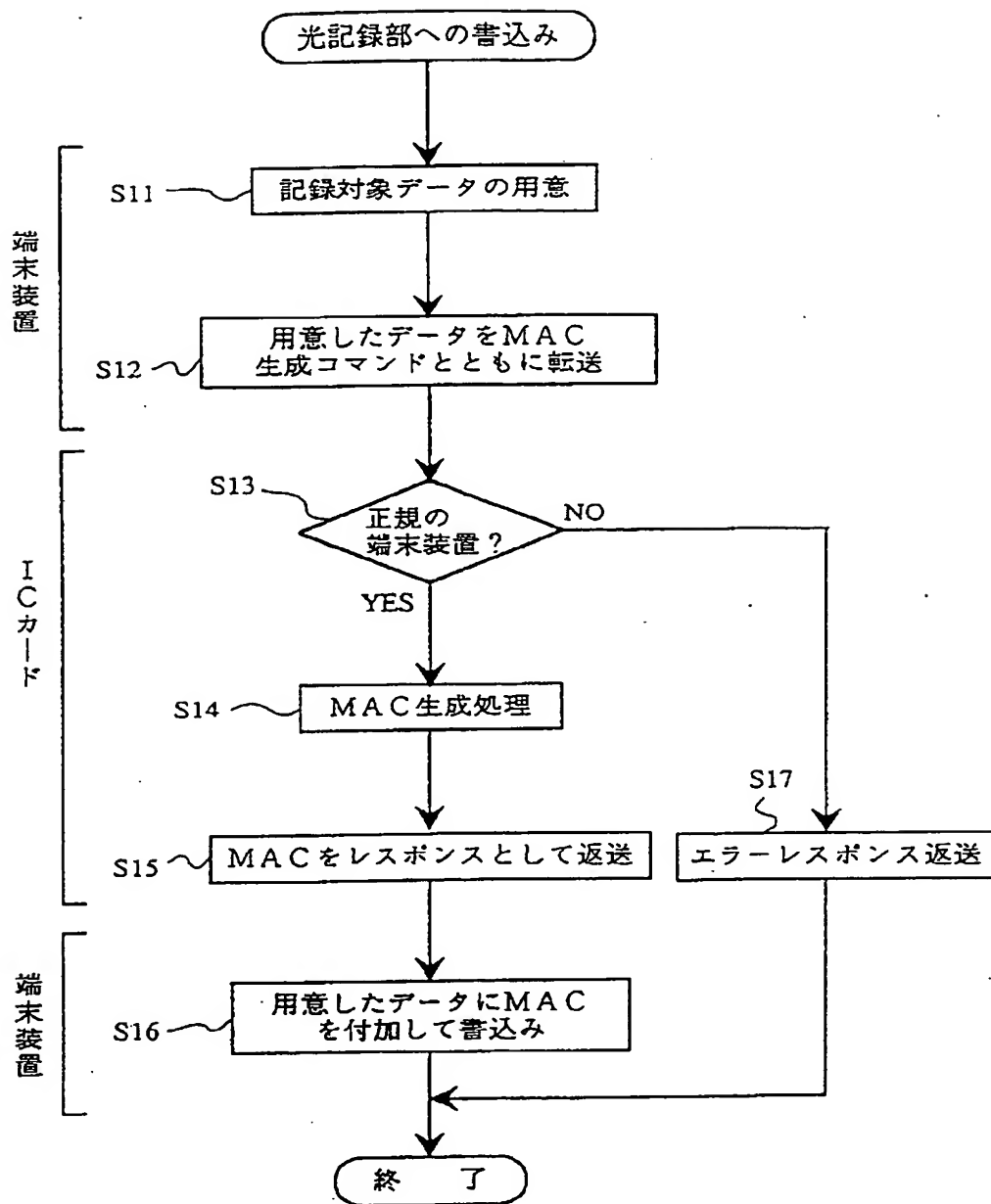
【図8】



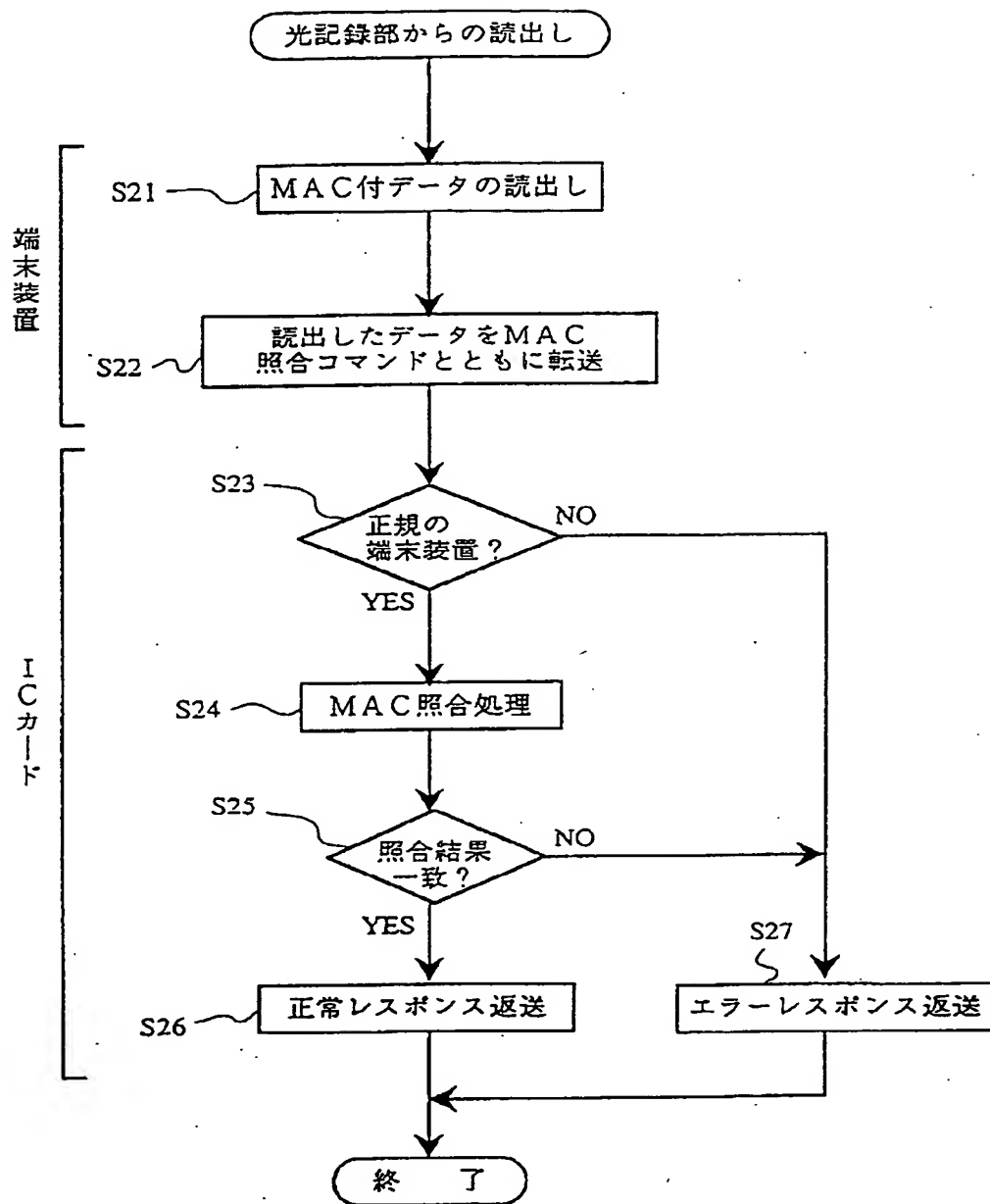
【図3】



【図5】



【図6】



【手続補正書】

【提出日】平成9年3月18日

【手続補正1】

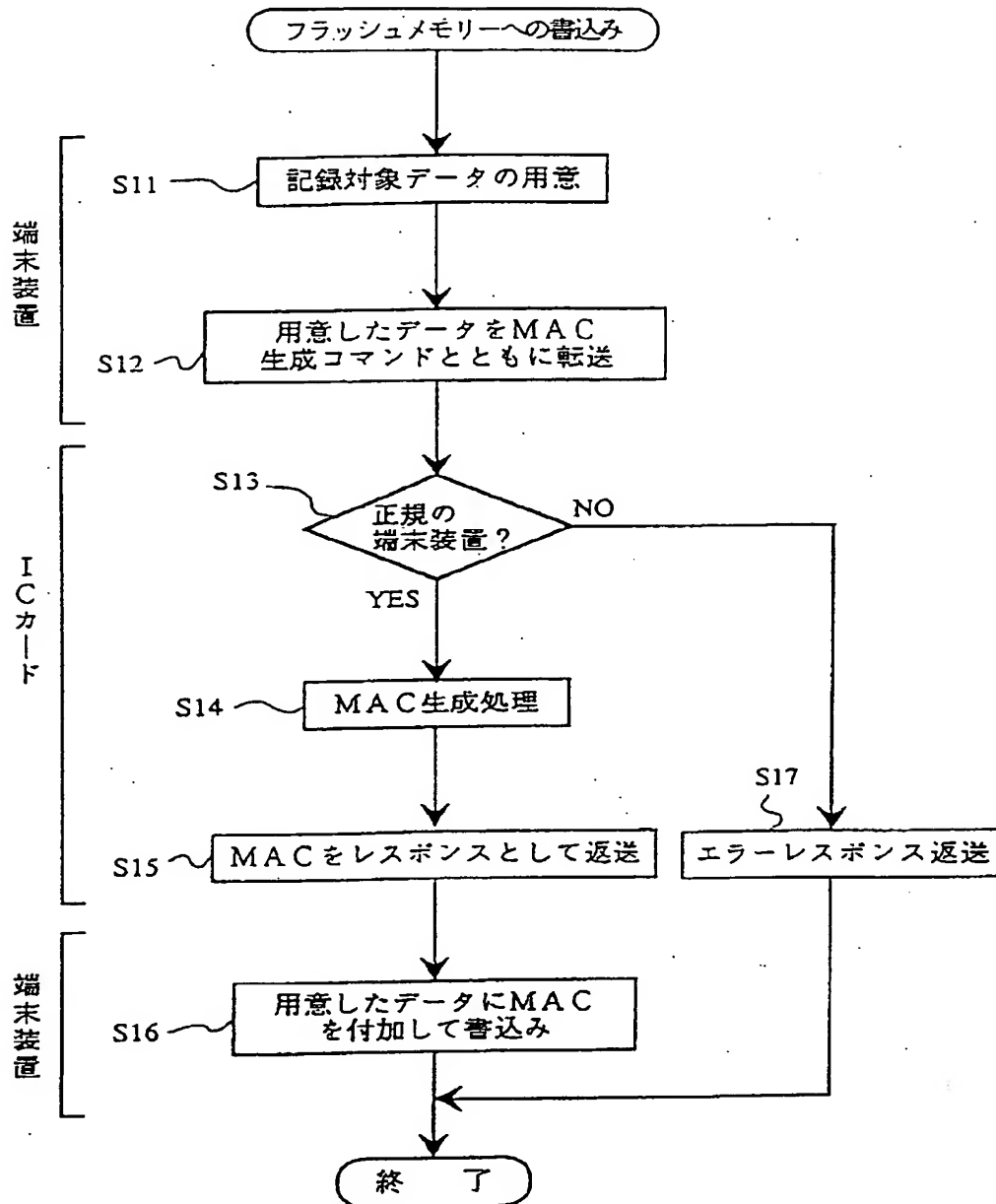
【補正対象書類名】図面

【補正対象項目名】図5

【補正方法】変更

【補正内容】

【図5】



【手続補正2】

【補正対象書類名】図面

【補正対象項目名】図6

【補正方法】変更

【補正内容】

【図6】

